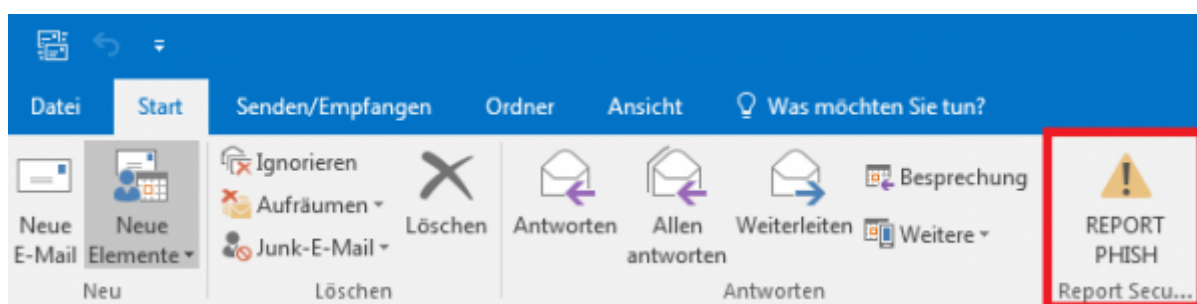


# Introduction

LUCY comes with a "Phish Alert" plugin/addon for mail clients or browsers:

- Outlook 2010
- Outlook 2013
- Outlook 2016
- Outlook 2019
- Office365 Desktop
- Office365 Web
- Office365 Mobile
- Outlook for Mac
- Office for Mac 2016
- Office for Mac 2019
- Gmail

This add-in gives your users a safe way to forward suspected Emails with only one click and have them analyzed automatically by the [Threat Analyzer](#) in LUCY. The tool empowers users to proactively participate in an organization's security program and makes it easy for your employees to report any suspicious email they receive. It has two main features



a) Forward the mail (.msg) to a predefined mail address (e.g. your security team). Within the plugin you have the ability to define a custom message that appears to the user after the mail gets reported. Once the message gets forwarded to your team, it will automatically be deleted from the user's inbox to prevent future exposure.

b) Report back to LUCY: the plugin may forward suspected phishing emails as well LUCY generated emails back to the LUCY server via HTTPS. If the mail was generated by LUCY, the reports will automatically be processed within the campaign statistics. All other emails can be analyzed in LUCY using our threat analysis engine.

There are 3 variations of the Report Plugin by design:

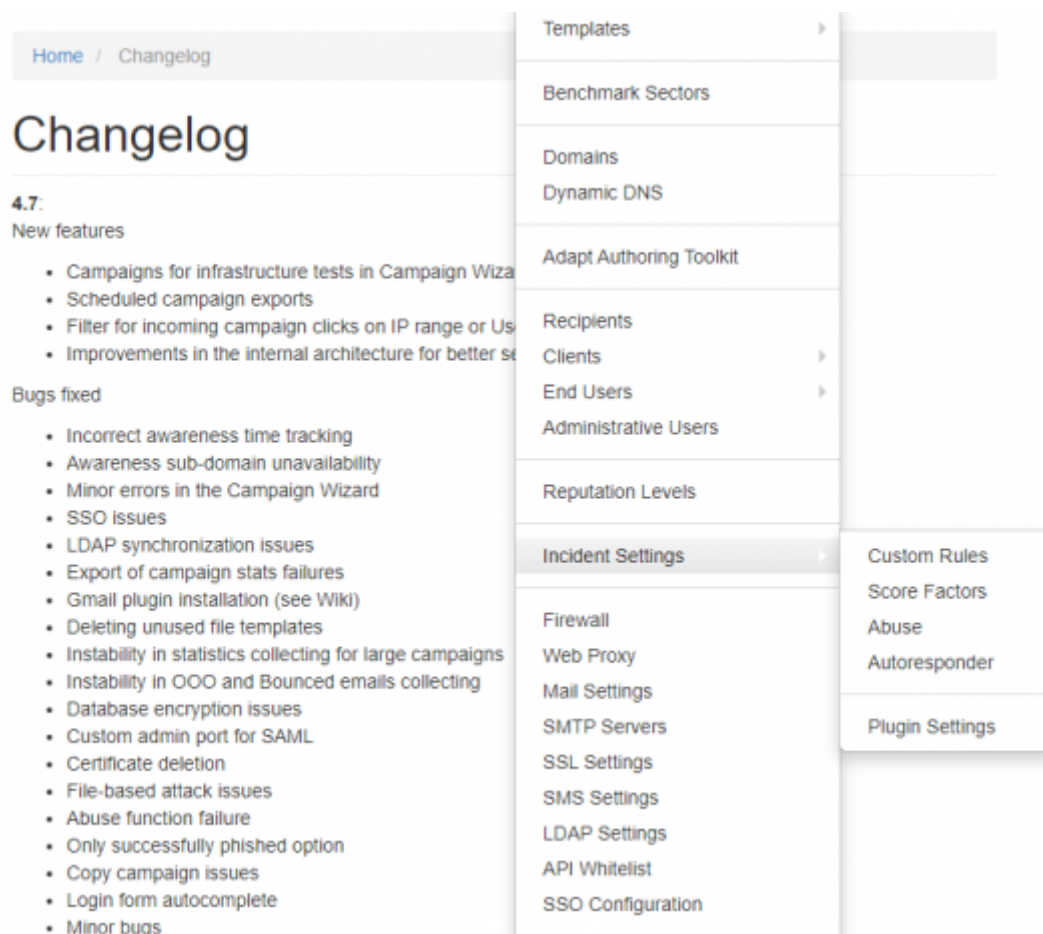
- [Outlook Plugin](#)
- [O365 Plugin](#)
- [Gmail Plugin](#)

## Configuration

## Incident Settings


The configuration of the plugin and phishing incidents is done within the settings menu (**Admin/Settings/Incident Settings**) where you can define the settings for:

- Custom Rules (create special rules with Regex filters to flag emails)
- Score Factors (adjust the scores for specific incident events)
- Abuse
- Autoresponder
- Plugin settings



## Plugin settings

The following settings can be configured:

Default Language	<div>English</div>	
Email	<div>plugin@lucysecurity.com</div>	?
	<div>Download Sample Icons</div>	
Outlook MSI Icon (ico)	<div>Choose File No file chosen</div>	?
	<div></div>	
	<div>Delete MSI Icon</div>	
Outlook O365 Icon (png)	<div>Choose File No file chosen</div>	?
	<div><input checked="" type="checkbox"/> Send Reports Over HTTP</div>	
	<div><input type="checkbox"/> Never report phishing simulations</div>	
	<div><input checked="" type="checkbox"/> Send Reports Over SMTP</div>	
	<div><input type="checkbox"/> Use SMTP for receiving incident reports on Lucy</div>	
	<div><input type="checkbox"/> Never report phishing simulations</div>	
	<div><input type="checkbox"/> Send phishing simulations Over HTTP</div>	
	<div><input type="checkbox"/> Use X-Headers in forwarded emails</div>	
	<div><input type="checkbox"/> Inline Message Forwarding ?</div>	
	<div><input checked="" type="checkbox"/> Deeper Analysis Request</div>	
	<div><input checked="" type="checkbox"/> Enable Comment to Deeper Analysis Request</div>	
	<div><input type="checkbox"/> Send reported mail attachment in EML format</div>	
	<div><input checked="" type="checkbox"/> Disable Autoresponder For Reports</div>	
	<div><b>Actions with reported emails</b></div>	
	<div><input checked="" type="radio"/> Delete reported email</div>	
	<div><input type="radio"/> Move reported email to non-system folder named</div>	
	<div></div>	
	<div><input type="radio"/> Move reported email to Junk E-mail of the current user</div>	
	<div><input type="checkbox"/> Notify of Expired Incidents ?</div>	

## Plugin Variations Feature Support Comparison

### Main Settings

Setting Name	Description	Outlook (MSI)	Office365 (XML)	Gmail
Default Language	Set the default language for the plugin.	+	+	+
Email	the mail address of your security team. This is the address, where suspected phishing mail gets forwarded. The whole mail will be attached as a .msg (for MSI plugin only) and send to a predefined mail address. You may use multiple emails separated by a semicolon symbol (;). Example: john@doe.com;bill@gates.com.	+	+	+
Outlook MSI Icon (ico)	Choose an icon for a visual representation of plugin's button in the Outlook MSI interface. Once it has been picked up there is a preview and an option to delete icon.	+	-	-
Outlook O365 Icon (png)	Choose an icon for a visual representation of plugin's button in the Office365 Outlook interface. Once it has been picked up there is a preview and an option to delete icon.	-	+	-
Send Reports Over HTTP	Enable this option, if you want the Outlook Plugin to send a copy of the reported phishing mail to LUCY (does not include emails from phishing simulations) and additionally add the statistical info about reported phishing emails to LUCY.	+	+	+
Never report phishing simulations	No reports will be sent over HTTP if user reports a simulation email generated by Lucy. So the plugin will send only "real phishing" emails over HTTP.	+	+	-
Send Reports over SMTP	Enable this option, if you want to forward the mail to the predefined mail address via SMTP. If enabled, the plugin will send the report to the email you provided on the same page. That is supposed to be your own email or the email of your security team. Please do not use this method at the same time with HTTP to send reports to LUCY, if you do not want to have duplicated reports. Only pick one delivery method.	+	+	+
Use SMTP for receiving incident reports on Lucy	if enabled, Lucy will suppose it has to intercept emails that plugin sends over SMTP, so it configures the local postfix accordingly. All emails received will be added to incidents. If you do not enable this, even if the email configured points to Lucy, nothing will happen - Lucy won't wait for reports over SMTP. This option requires that the first e-mail in the "Email" field should be the e-mail of Lucy postfix server	+	+	+
Never report phishing simulations	No reports will be sent over SMTP if user reports a simulation email generated by Lucy. So the plugin will send only "real phishing" emails over SMTP. If HTTP is disabled as well, Lucy will not get these reports either, as there is no other delivery method configured for these reports.	+	+	+

Setting Name	Description	Outlook (MSI)	Office365 (XML)	Gmail
Send phishing simulations over HTTP	If the option is enabled, the plugin will send reports regarding phishing simulations to LUCY via HTTP.	+	+	-
Use X-Headers in forwarded emails	If true, the plugin will make the following changes in the email forwarded over SMTP: * Add a new header X-CI-Report: True * Add a HTML code <p>X-CI-Report: True</p> after the body tag within the email body.	+	+	-
Inline Message Forwarding	If true, the plugin will clear the body of the forwarded email when sending the report via SMTP.	+	-	-
Deeper Analysis Request	If true, the plugin will ask the user whether to request deeper analysis of the reported phishing mail.	+	+	-
Enable Comment to Deeper Analysis Request	If Deeper Analysis Request is true, the plugin will offer to the user an additional text box where the user can type any comment to the deeper analysis request. Additionally the user can configure a custom text that will appear instead of "Yes" or "NO" labels on the buttons	+	-	-
Send reported mail attachment in EML format	Reported email message will be sent as an *.eml attachment.	+	+	+
Disable Autoresponder For Reports	If true, LUCY will not send an automatic email to a user as a reaction to report.	+	+	+
Delete reported email	Set this action option and the plugin will delete the reported emails.	+	-	-
Move reported email to a non-system folder named	Set this option and the plugin will move reported emails to the custom-named folder. Type in the folder name in the field below.	+	-	-
Move reported email to Junk E-mail of the current user	Set this action option and the plugin will move reported email to Junk E-mail of the current user.	+	-	-
Notify of Expired Incidents	Check this to receive notification if there are reports older than 30 days. This notification will be delivered via email.	+	+	+

## Language Settings

Language settings are required to be configured before the initial download of the plugin from the Incidents Tab.

The language sample text (English) can be found [here](#).

Please note, multi-language support is only available for the MSI plugin. The locale will be set automatically according to the Outlook's language. Otherwise the default language will be used.

# Language Settings

[Settings](#)
[Language Settings](#)

**Language**

**Thank You Message**

**Thank You Message For Lucy Emails**

**Button Message**

**Button Super Tip**

**Report Title**

**Error Title**

**User Request Message**

**Deeper Analysis Request Message**

**No Selection Message**  ?

**Eval Error Message**  ?

**Send Error Message**

**Unsupported Message**  ?

**Subject**  ?

**Ribbon Label**  ?

**Deeper Analysis Request Custom Buttons**

**For "Yes" action**

**For "No" action**

Setting Name	Description	Outlook (MSI)	Office365 (XML)	Gmail
Language	Choose the language preset to configure it specifically for the needed language.	+	+	+
Thank you message	The message that will be displayed after the user marks a suspected phishing email and pushed the plugin button.	+	+	-
Thank you message for LUCY mails	The message that will be displayed for all emails, that are created by LUCY within a simulated phishing campaign.	+	+	-

Setting Name	Description	Outlook (MSI)	Office365 (XML)	Gmail
Button Message	The name of the button in Outlook.	+	-	-
Button Super Tip	The help text displayed when the user hovers the mouse over the button.	+	-	-
Report Title	The title of the message that will be displayed after the user marks a suspected phishing email and clicks the plugin button.	+	+	-
Error Title	The title of the message that will be displayed when any error occurs.	+	+	-
User Request Message	The message that will be displayed after the user marks a suspected phishing email and clicks the plugin button.	+	+	-
Deeper Analysis Request Message	Deeper analysis request confirmation text. This message box is shown after user clicks on the report button.	+	+	-
No Selection Message	The title of the message that will be displayed after the user clicks phish button without any selected email.	+	-	-
Eval Error Message	Text displayed when the error of getting the selected item occurs.	+	-	-
Send Error Message	The message that will be displayed when an issue with sending the report occurs.	+	-	-
Unsupported Message	Text displayed when user tries to report an unsupported item (calendar event, etc).	+	-	-
Subject	The subject of the forwarded email message when sending a report over SMTP. You may use %subject% variable to insert the subject of the phishing email. Example: Phish Alert %subject%.	+	-	+
Ribbon Label	The name of the area in which the button is located.	+	-	-
For "Yes" action	Set the Deeper Analysis Request Custom Button for "Yes" action.	+	+	-
For "No" action	Set the Deeper Analysis Request Custom Button for "No" action.	+	+	-

The algorithm logic for the different delivery options in the plugin is as follows:

1. Is HTTP enabled? If yes, send a report over HTTP, regardless of its status (simulation or real)
2. Is SMTP enabled? If no, stop, otherwise go to next
3. Is "Never report phishing simulations (Suppress SMTP)" enabled AND this is a simulation email?  
If BOTH are yes, then stop, otherwise go next
4. Send report over SMTP

For more clarification of various use cases of the plugin configuration please refer to the examples [here](#).

**Known Issues:** if you use SMTP for receiving incident reports on Lucy within the incidents, Lucy will intercept all your emails to the domain specified. If you use example.com as a domain for receiving the incidents in LUCY, the internal Postfix server will be listening for this domain for incoming mails. If you now start at the same time a phishing or awareness campaign and try to send your emails to "@example.com", LUCY will not forward those emails externally.

## Phishing Incident Center Features (Threat Analyzer)

Phishing Incident Reports created by users are collected in the Incidents section.

- **Dashboard Filter:** LUCY allows you to filter the incoming mails on the dashboard:

The screenshot shows the 'Phishing Incident Reports' dashboard. At the top, there are buttons for 'Send Abuse', 'Delete', 'Delete All', 'Change Status', and 'Download Plugin'. Below these is a 'Filter' dropdown menu, which is highlighted with a red box. The filter menu is open, showing options: 'All', 'Open', 'In Progress', 'Dismissed', 'Simulation', 'Real Phishing', and 'Closed'. The 'All' option is currently selected. Other filter fields include 'Search', 'Client' (set to 'All'), 'Email Domain' (set to 'All'), 'Campaign' (set to 'N/A'), 'From Date' (08/20/2019), 'To Date' (08/20/2020), 'Score type', and 'Min value'. An 'Update' button is located below the filter fields. A 'Statistics' dropdown is visible at the bottom left of the filter section.

- **Centralized Analysis:** This feature allows you to analyse the incoming mails manually or automatically
- **Centralized Campaign Reporting:** Any reported mail which is part of a phishing simulation will be processed within the campaign statistics
- **Threat Mitigation:** The Threat Mitigation allows you to take actions against legitimate phishing attacks
- **Custom Regex & Score:** LUCY allows you to define custom rules to scan mails for specific keywords and flag them with a individual threat score.

### Detection of real phishing mails vs. Phishing simulations

The plugin automatically handles emails created in a phishing simulations from LUCY: it will ensure that only reports of potentially malicious emails are delivered to appropriate security staff. All emails created by LUCY itself will create a custom message to inform the user, that the mail has been send as a part of a security awareness program. LUCY generated phishing mails won't be forwarded to the security team. But they will be reported back to LUCY in order to process the information within the campaign statistics. The reported mails will then be purged from the successful attack listings in LUCY.

### Where are incidents (LUCY generated emails) from the plugin reported?

If a user spots the phishing simulation and reports the email, you can see this information in various places:

- Incident widget on the dashboard:



Home / Campaigns

## Campaigns

+ New Export Select All Actions Type-Based Add Widget

**Statistics Phish Alert**

Users reported a real phishing mail:	24
Users reported a phishing simulation mail:	4
Average response time (days):	0

- Incident tab:

UPDATE SERVER Campaigns **Incidents** Settings Support Tools

Home / Phishing Incident Reports

## Phishing Incident Reports

Send Abuse Delete Delete All Change Status Download Plugin

Filter

Statistics

<input type="checkbox"/>	Time	Email	Client	Campaign	Score	Status	
<input type="checkbox"/>	08/17/2020 15:17		A	5522 (1)	0.00	Simulation	
<input type="checkbox"/>	08/17/2020 14:08		N/A	N/A	10.00	Open	

- Under the campaign statistics (recipients) under the "reported" item:

Results

Search...

Summary

Statistics

File Downloads

Collected Data

**Recipients**

Awareness Website

Benchmark

Compare

Reports

Exports

100% 4 Recipients

100% 4 Sent

25% 1 Opened

25% 1 Clicked

0% 0 Vulnerable

25% 1 File Downloaded

25% 1 Data Submitted

Name	OS	UA	Plugins	Succ	Train
<input type="checkbox"/> Oliver Muenchow Login	-	-		-	-
<input type="checkbox"/> Oliver Login	-	-		-	-
<input type="checkbox"/> Kadau Login	-	-		-	-
<input type="checkbox"/> <u>Oliver Muenchow</u> Login	Windows 7	MSIE 11		✓	-

**Name** Oliver Muenchow

**E-mail** oliver@kunstwarenhaus.ch

**Phone** -

**Plugins** Silverlight Plug-In 5.1.50907.0

**Vulnerable Applications (0)** N/A

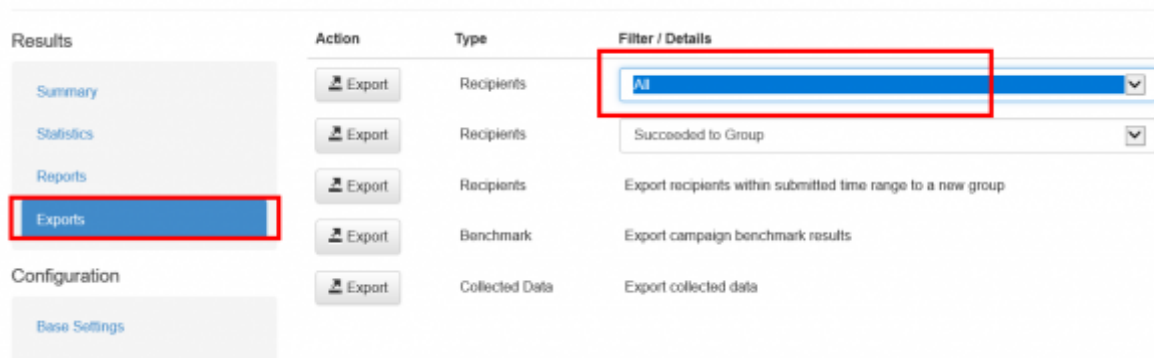
**Lure Sent** -

**Message Sent** 05/08/2018 16:20:22

**Training Sent** -

**Reported** -

- If you want a comparison of all reported emails, you can export the whole campaign data via CSV. Within the CSV there is a reported column:



The incidents reports will also be integrated on the dashboard under the general statistics.

For more detailed information on the report's analysis please proceed to [Centralized Analysis](#).

## Threat mitigation

The threat mitigation allows a LUCY admin to report reported phishing mails to according abuse contact of the provider's originating IP address taken from the message header. You can click on the mail symbol within the incident center to initiate the sending of the report. More info [here](#).

## API Integration

The e-mails reported to LUCY via plugin can be automatically forwarded to external systems (e.g. Splunk) via LUCY's [REST API](#). This ensures a seamless connectivity to a SOC.

## Technical Details

The plugin is a non signed MSI file and programmed as a C++/COM object. It is bundled with Microsoft Visual C++ 2015 Redistributable (x86) Package (14.0.23026). The loading time of the plugin is around 10 MS. It has been tested in Outlook 2010, 2013 & 2016. An Office365 and Gmail Plugins are also available.

A phishing mail generated in LUCY will have a "X-Lucy-VictimUrl" value in the mail Header. This allows LUCY to identify the phishing mail and Report it back to the app using a HTTPS call. Example:

X-Lucy-VictimUrl: <https://microsoft.secure-log-in365.info/f56/phishing-report> Message-Id: 20170414072426.390935E2095F@demo.phishing-test.services

If the user clicks the phish button where the HTTP delivery is configured in the Settings, a new click Event is generated. The variables could look like this:

```
url: https://demo.phishing-test.services/phishing-report
email: test@lucysecurity.com
message: Thanks. Your help is appreciated!
lucyMessage: This was a phishing simulation. Thank you for your help!
buttonText: Phish Reporter
```

```
submitHttp: yes
submitSmtP: yes
something is selected
user clicked yes
property accessor is ok
submitting over smtp...
successfully submitted over smtp
submitting over http...
  url: https://microsoft.secure-log-in365.info/f56/phishing-report
```

**HTTPS communication - plugin to LUCY:** The XML always uses web browser to send data to Lucy. In case of running as a web-plugin in MS Outlook it uses the build-in web browser (for Windows it is Internet Explorer) to communicate with Lucy. Both, MSI and XML, use the proxy system settings (Windows > Control Panel > Network and Internet > Internet Options). If Windows-based authentication is required for the proxy, it will work transparently as well as for MSI and XML.

## Using your own plugin to report emails to LUCY

There is a possibility to use your own plugin to report emails to LUCY. To do this you need:

1. Configure your domain that is used for LUCY so that its MX records might point to LUCY
2. Configure an email address for receiving incident reports in Settings - Incidents Settings - Plugin Settings, this email address should use the domain configured on step 1.
3. Turn on check-boxes "Send Reports Over SMTP" and "Use SMTP for receiving incident reports on LUCY"

After these steps are done you can forward any email as an attachment to the configured email address and LUCY will treat these emails as incident reports and display them on the "Incidents" page.

## Potential Issues

If you enable "send reports via SMTP" you cannot send emails to the same domain (e.g. "example.com") anymore: this setting will cause Lucy to intercept all your emails to "example.com" domain. If you remove the checkbox, then Lucy won't try to intercept emails for that domain and the feature will work as expected. Using "Send Reports Over SMTP" along with "Use SMTP for receiving incident reports on Lucy" is the other way to deliver phishing reports to Lucy. You can specify, for example, some custom email like [lucy-phishing-reports@separatedomain.com](mailto:lucy-phishing-reports@separatedomain.com) as a primary email in Incidents settings, check both those checkboxes and point [separatedomain.com](https://separatedomain.com) MX records to Lucy. So all emails being sent to [lucy-phishing-reports@separatedomain.com](mailto:lucy-phishing-reports@separatedomain.com) will be intercepted by Lucy, as well as emails sent from Outlook plugin - they will be added to the "Incidents" page. If you just want to receive a copy of incident report to your own email ([yourname@example.com](mailto:yourname@example.com)), that is not tied to Lucy, then you should keep "Use SMTP for receiving incident reports on Lucy" checkbox clear - in that case Lucy won't attempt to intercept anything and the plugin will just forward all reports to [yourname@example.com](mailto:yourname@example.com).

From:

<https://wiki.lucysecurity.com/> - **LUCY**

Permanent link:

[https://wiki.lucysecurity.com/doku.php?id=phishing\\_incidents](https://wiki.lucysecurity.com/doku.php?id=phishing_incidents)

Last update: **2022/01/18 09:02**

